NetIQ CloudAccess and NetIQ MobileAccess 2.3 SP1 Release Notes

March 2016

NetIQ CloudAccess is an appliance that provides a simple, secure way to manage access to Software-as-a-Service (SaaS) applications for corporate users. It provides out-of-the box security and compliance capabilities for SaaS services including full user provisioning, dynamic credentialing, privileged user management, single sign-on (SSO), and compliance reporting.

NetIQ MobileAccess is an appliance that enables user access to protected resources from mobile devices. It provides convenient access for users, as well as the ability for administrators to customize viewing options and remotely manage registered devices.

This service pack improves usability and resolves several previous issues. Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the CloudAccess forum (https://forums.netiq.com/forumdisplay.php?118-CloudAccess) on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the NetIQ CloudAccess Documentation (https://www.netiq.com/documentation/cloudaccess/) page. To download this product, see the NetIQ Downloads (https://dl.netiq.com/) website.

1 What’s New?

The following sections outline the key features and functions provided by this version, as well as issues resolved in this release.

1.1 Operating System Updates

This service pack for CloudAccess and MobileAccess includes various operating system updates.

1.2 Enhancements and Software Fixes

CloudAccess includes the following enhancements and software fixes:

1.2.1 OpenSSL Update

This service pack includes update OpenSSL 1.0.1s, which includes a fix for the “DROWN” vulnerability. For more information, see CVE-2016-0800 (https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0800).

For more information about all fixes included in the OpenSSL 1.0.1s update, see the following: https://openssl.org/news/secadv/20160301.txt (https://openssl.org/news/secadv/20160301.txt).

1.2.2 Updated MobileAccess App

This version includes an updated version of the MobileAccess app for supported mobile devices.

1.2.3 Portal Page Issue

When proxying the portal page through NetIQ Access Manager, the portal page failed to render completely. After you install this service pack, the portal page renders correctly. (Bug 963518)

[Return to Top]

2 System Requirements

If you have an existing installation of CloudAccess or MobileAccess 2.3 Hotfix 1 (2.3.0-235), you can update your appliance through the update channel. Or, you can upgrade your environment by installing a new appliance in the cluster, allowing the information to synchronize, and then deleting the old node in the cluster.

You can also install this service pack in a new environment using the OVF file, available from the NetIQ Downloads web page (https://dl.netiq.com/).

For detailed information on hardware requirements and supported operating systems and browsers, see “Installing the Appliance” in the *NetIQ CloudAccess and MobileAccess Installation and Configuration Guide*.

[Return to Top]

3 Installing or Updating the Appliance

To update an existing CloudAccess or MobileAccess appliance through the update channel, see “Updating the Appliance” in the *NetIQ CloudAccess and MobileAccess Installation and Configuration Guide*.

The steps for installing and configuring the appliance in a new environment are the same for CloudAccess and MobileAccess. For more information, see “Installing the Appliance” in the *NetIQ CloudAccess and MobileAccess Installation and Configuration Guide*.

[Return to Top]

4 Verifying the Installation or Update

Perform the following steps to verify that the installation or update was successful.

To check the installed version:

1. Access the administration console at `https://dns_of_appliance/appliance/index.html`, then log in with the appliance administrator credentials.
2. Click the appliance, then click **About**. Verify that the version listed in the window is `2.3.1-7`.

[Return to Top]

5 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support (http://www.netiq.com/support).

5.1 Initialization and Administration Issues

5.1.1 Changes to the Preferred DNS Server During Initialization Result in a Static IP Address

Issue: If you want to change the preferred DNS server, you must select **Use the following IP address** in Step 1 on the initialization page, which assigns a static IP address to the appliance. (Bug 754137)

Workaround: After the initialization process completes, on the Admin page, change the IP address from static to DHCP.

5.1.2 Modifying a Non-Public SSL Certificate on the External Filter Server Causes User Logins to Fail Until the Next Apply

Issue: If you modify a non-public SSL certificate (that is, a certificate that has not been signed by a well-known certificate authority) on the external filter server, the login service does not automatically re-read the trust store. User logins fail with a message that an external service is unavailable. However, the health status does not detect this failure and reports a healthy (green) status. This condition does not occur if you modify a certificate from a well-known certificate authority on the filter server. (Bug 895375)

Workaround: If you modify a non-public SSL certificate on a filter server, you must click **Apply** to restart the login services in the cluster, or reboot the appliance. A restart causes the login service to re-read the trust store and get the new certificate information. After the restart, users can log in again.

5.1.3 Page Becomes Unresponsive When You Approve Requests

Issue: When you approve or deny a large number of workflow requests in a single action, the amount of memory that the browser uses can cause the page to become unresponsive and the browser to close. (Bug 815971)

Workaround: Ensure that you select less than 300 requests in a single accept or deny action.

[Return to Top]

5.2 Provisioning Issues

5.2.1 Provisioning Is Not Supported for Users in an Unmanaged SAML2 In Identity Source

Issue: Account provisioning is not supported for the users in the SAML 2.0 Inbound unmanaged internal identity store. Because these users do not have a workforceID, they cannot be provisioned for or access the SaaS applications that depend on the workforceID attribute for authentication, such as Google Apps and Salesforce. (Bug 883446)

Workaround: To access the SaaS applications, the user must log in with the corporate identity that has a workforceID attribute.

5.2.2 User Email Address Changes in Active Directory Are Not Provisioned to Salesforce

Issue: User email address changes in Active Directory are not provisioned to Salesforce. (Bug 717153)

Workaround: No workaround is available at this time.

5.2.3 Re-enabled User Has Role That Was Previously Assigned

Issue: If you assign a user to a role in CloudAccess and then remove that user from the identity source, CloudAccess does not automatically remove the role assignment. If the user's context in the identity source is later restored, CloudAccess shows that user as having the same role that was previously assigned. (Bug 765609)

Workaround: To work around this issue, before you remove a user in the identity source, ensure that you have revoked all roles from that user on the Roles page in CloudAccess.

5.2.4 Non-Alphanumeric Characters in the Group Description Result in Users Seeing No Appmarks

Issue: If you use non-alphanumeric characters (such as !@#$%) in a group description, policy mapping may appear to be successful, but users in that group do not see the mapped appmarks. (Bug 922124)

Workaround: Remove any non-alphanumeric characters from the group description.

5.2.5 SAML 2.0 Inbound Users See Only Public Access Appmarks

Issue: When using the SAML 2.0 Inbound connector in mode **Allow access for unknown users**, after the first login when the user has just been created, the landing page displays only the Public appmarks. (Bug 920022)

Workaround: Since these specific types of users are not stored locally on the appliance, the appliance cannot apply the proper roles until the user logs in a second time. If you have any users that see this problem, instruct them to log out and log back in to the landing page. The landing page properly displays all of the appmarks.

5.2.6 SAML 2.0 Inbound Users Using Kerberos and TOTP Cannot Access Simple Proxy or OAuth Appmarks

Issue: When you have enabled Kerberos and Google TOTP on the Simple Proxy and OAuth appmarks, and SAML 2 Inbound users are in the mode **Allow access for unknown users** or **Allow access for known users**, the users cannot access the appmarks. When users click the Simple Proxy or OAuth appmarks, CloudAccess presents to them a second login screen. Since the users are already authenticated, CloudAccess cannot log in the SAML 2 Inbound users again. (Bug 923207)

Workaround: Do not use Google TOTP and Kerberos with SAML 2 Inbound users.

5.2.7 Cannot Set Search Context to Root of Active Directory

Issue: If you set the search context on a connector for Active Directory to the root of your AD identity source, CloudAccess displays an exception error and does not import all users. (Bug 956310)

Workaround: Do not set the search context for the connector for Active Directory to the root of your AD identity source.

5.2.8 Cannot Use Case Exact Attributes with User or Group Filtering

Issue: When using the user or group filtering option with an LDAP identity source, using case exact attributes does not work for values with any uppercase characters. (Bug 935967)

Workaround: If you are searching for a custom attribute, ensure that when you create the attribute, you create the attribute with the option **Case Ignore String**. Otherwise, there is no workaround at this time.

5.2.9 Cannot Change User or Group Filter and Change Naming Attribute in Same Operation

Issue: If you change the user or group filter to exclude some users from an LDAP identity source, and you change the naming attribute in the same operation, both the rename and the user filtering fail. (Bug 936298)

Workaround: Instead of performing both actions in the same operation, change the filter, wait for the sync, then change the naming attribute and wait for the sync.

[Return to Top]

5.3 Reporting Issues

5.3.1 Reports Display Information from Deleted Connectors

Issue: After you delete connectors, reports still contain information about the deleted connectors. (Bug 756690)

Workaround: No workaround is available at this time.

5.3.2 Mapping Report Displays Numeric Values Appended to Data in the Authorization Name Column

Issue: The numeric value in the mapping report appears after deleting and recreating mappings for connectors. (Bug 753321)

Workaround: No workaround is available at this time.

[Return to Top]

5.4 Connector Issues

5.4.1 Logging Out of Identity Provider Landing Page Does Not Result in Logging Out of SaaS Accounts

Issue: Logging out of the landing page might not result in logging out of the SaaS accounts, depending on support and configuration for SAML Single Logout at the SaaS provider. Many SaaS providers do not support the SAML Single Logout service. The same issue exists with service provider-initiated logouts. (Bug 837076)

Workaround: Close the browser to allow the abandoned browser session to time out, so the session cannot be accessed again.

5.4.2 Admin Page Does Not Provide a Way to View SaaS Metadata

Issue: The Admin page in CloudAccess does not currently provide a means of viewing the critical content in an uploaded metadata file, such as when you configure the connector for Salesforce. (Bug 793495)

Workaround: No workaround is available at this time. Since metadata for connectors must be unique, ensure that the metadata file is correct before uploading it.

5.4.3 Renaming an Authorization for an Office 365 Account Requires Policy Remapping in CloudAccess

Issue: If an authorization at the Office 365 account is renamed, any existing policy mappings in CloudAccess are lost, because CloudAccess uses the account name for policy mapping rather than the underlying static ID of the authorization. If you rename an authorization in Office 365, CloudAccess sees the action as a delete and create, and removes any existing policy mappings for the authorization. (Bug 811460, 815496)

Workaround: After changing the authorization name in Office 365, use the Policy page to re-map entitlements for the renamed authorization, and then use the Approval page to re-approve, if necessary.

5.4.4 Users Who Are Provisioned to Multiple Google Domains Cannot Access Original Mailbox

Issue: If you provision a user to multiple Google Apps domains and select the **Enable email proxy** option in the administration console, the user cannot open the mailbox for any domain except the last domain to which the user was provisioned. This issue occurs because the embedded mail proxy in the appliance uses an attribute from the user object that is single-valued, so it is set with the name of the last Google domain to which the user was provisioned. (Bug 819157)

Workaround: No workaround is available at this time.

5.4.5 Connector for NetIQ Access Manager Tries to Import Certificate with the Same Name Every Time

Issue: The connector for NetIQ Access Manager tries to import the certificate to NetIQ Access Manager with the same name every time. If you remove the connector, the imported certificate to NetIQ Access Manager is not removed. So, the next time you create a connector for NetIQ Access Manager for the same Access Manager system, it fails unless the certificate is the same certificate. (Bug 923217)

Workaround: To work around this issue, before you create a new connector for NetIQ Access Manager in CloudAccess, delete the previous certificate in the Access Manager administration console.

5.4.6 Cannot Authenticate to Advanced Authentication Framework 5.2

Issue: You have configured the Advanced Authentication Framework method to work with Advanced Authentication Framework 4.2. After completing the configuration, you try to authenticate with an Advanced Authentication Framework method and it fails.

Workaround: The Advanced Authentication Framework changed with the 5.2 release. You must manually enable endpoints on the Advanced Authentication Framework system to make authentications work.

To configure endpoints in the Advanced Authentication Framework administration console:

1. Log in to the administration console for Advanced Authentication Framework as an administrator.
2. From the left navigation pane, click **Endpoints**.
3. Select the **Endpoint41** endpoint.
4. Click the Pencil to edit the endpoint, then enable the endpoint.
5. Save your changes.

Authentications through the Advanced Authentication Framework methods now work.

[Return to Top]

6 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com (mailto:Documentation-Feedback@netiq.com). We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website (http://www.netiq.com/support/process.asp#phone).

For general corporate and product information, see the NetIQ Corporate website (http://www.netiq.com/).

For interactive conversations with your peers and NetIQ experts, become an active member of our community (https://www.netiq.com/communities/). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

[Return to Top]

7 Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/. All third-party trademarks are the property of their respective owners.

[Return to Top]